CLAIMS

1. A document security system for restricting access to documents, said document security system comprising:

at least one process-driven security policy that includes a plurality of states and transition rules, each of the states having corresponding one or more access restrictions, and the transition rules specify when the secured document is to transition from one state to another; and

an access manager that determines whether access to a secured document is permitted by a requestor based on the state and the corresponding one or more access restrictions thereof for said process-driven security policy.

2. A document security system as recited in claim 1, wherein the corresponding one or more access restrictions for access to the secured document are automatically changed when the state of said process-driven security policy for the secured document changes.

3. A document security system as recited in claim 1, wherein events cause the state of said process-driven security policy for the secured document to automatically transition between states.

4. A document security system as recited in claim 3, wherein the events are internal or external events with respect to said document security system.

5. A document security system as recited in claim 4, wherein at least one of the events is an external event from a document management system.

6. A document security system as recited in claim 1, wherein one or more of the corresponding one or more access restrictions for access to the secured document

remain intact when the state of said process-driven security policy for the secured document changes.

7. A document security system as recited in claim 1,

wherein events cause the state of said process-driven security policy to automatically transition between states,

wherein said process-driven security policy includes at least a first state, a second state, and a third state, and

wherein a first event causes transition from the first state to the second state, and a second event causes transition from the second state to a third state.

8. A document security system as recited in claim 1,

wherein events cause the state of said process-driven security policy to automatically transition between states,

wherein said process-driven security policy includes at least a first state and a second state, and

wherein a first event causes transition from the first state to the second state.

9. A document security system as recited in claim 1, wherein the transition rules are based on events.

10. A document security system as recited in claim 9, wherein the transition rules are written in XML.

11. A document security system as recited in claim 1,

wherein events cause the state of said process-driven security policy for the secured document to transition from a previous state to a current state, and

wherein the secured document is modified when said process-driven security policy for the secured document transitions from the previous state to the current state.

12. A document security system as recited in claim 11,

wherein the secured document includes at least a security information portion and an encrypted data portion, the security information portion including at least an encrypted key, and the key being encrypted must be decrypted in order to decrypt the encrypted data portion, and

wherein when said process-driven security policy for the secured document transitions from the previous state to the current state, the secured document is modified by decrypting the encrypted key and then re-encrypting the key, whereby the key is encrypted differently for the current state than the previous state.

13. A document security system as recited in claim 11, wherein, if permitted, access to the secured document is available at a client machine.

14. A method for transitioning at least one secured document through a security-policy state machine having a plurality of states, said method comprising:

(a) receiving an event;

(b) determining whether the event causes a state transition for the at least one secured document from a former state to a subsequent state of the security-policy state machine; and

(c) automatically transitioning from the former state to the subsequent state of the security-policy state machine when said determining (b) determines that the event causes the state transition.

15. A method as recited in claim 14, wherein the security-policy state machine implements a process-driven security policy, wherein each state of the security-policy state machine has different access restrictions.

16. A method as recited in claim 14, wherein each of the states of the security-policy state machine have different access policies.

17. A method as recited in claim 16, wherein the security-policy state machine is provided or part of a document security system, and wherein the different access policies of the security-policy state machine are enforced by the document security system.

18. A method as recited in claim 14, wherein said transitioning (c) comprises modifying the secured document to reflect the subsequent state of the security-policy state machine.

19. A method as recited in claim 14, wherein said transitioning (c) comprises:

retrieving an encrypted file key from the secured document;

decrypting, if permitted by the former state of the security-policy state machine, the encrypted file key to yield a file key;

subsequently encrypting the file key in accordance with the subsequent state of the security-policy state machine; and

storing the secured document, the secured document including at least an encrypted data portion and the subsequently encrypted file key.

20. A method as recited in claim 14, wherein said transitioning (c) comprises:

retrieving an encrypted file key from the secured document;

obtaining a private state key associated with the former state of the security-policy state machine;

decrypting the encrypted file key using the private file key;

obtaining a public state key associated with the subsequent state of the security-policy state machine;

subsequently encrypting the file key in accordance with the public state key; and

storing the secured document, the secured document including at least an encrypted data portion and the subsequently encrypted file key.

21. A method for imposing access restrictions on electronic documents, said method comprising:

providing at least one process-driven security policy at a server machine, the process-driven security policy having a plurality of states associated therewith, each of the states having distinct access restrictions;

providing a reference to the process-driven security policy at a client machine, the reference referring to the process-driven security policy resident on the server machine;

associating the reference to an electronic document;

transitioning the process-driven security policy from one state to a current state; and

subsequently determining at the server computer whether a requestor is permitted to access the electronic document, the access being based on a current state of the process-driven security policy, the current state being informed to the server computer by sending the reference to the server computer.

22. A method as recited in claim 21, wherein said transitioning is automatically performed based on events.

23. A method as recited in claim 22, wherein said transitioning is performed at the server machine.

24. A method as recited in claim 21, wherein said associating associates the reference to a group of documents.

25. A method as recited in claim 21, wherein said method pertains to a group of electronic documents, and wherein all of the electronic documents of the group are always in the same state of the process-driven security policy.

26. A method as recited in claim 21, wherein said determining comprises evaluating the process-driven security policy of an electronic document at the server computer based on at least the security policy restrictions for the current state of the process-driven security policy for the electronic document.

27. A computer readable medium including at least computer program code for transitioning at least one secured document through a security-policy state machine having a plurality of states, said computer readable medium comprising:

computer program code for receiving an event;

computer program code for determining whether the event causes a state transition for the at least one secured document from a former state to a subsequent state of the security-policy state machine; and

computer program code for automatically transitioning from the former state to the subsequent state of the security-policy state machine when said computer program code for determining determines that the event causes the state transition.

28. A computer readable medium including at least computer program code for imposing access restrictions on electronic documents, said computer readable medium comprising:

computer program code for providing at least one process-driven security policy at a server machine, the process-driven security policy having a plurality of states associated therewith, each of the states having distinct access restrictions;

computer program code for providing a reference to the process-driven security policy at a client machine, the reference referring to the process-driven security policy resident on the server machine;

computer program code for associating the reference to an electronic document;

computer program code for transforming the process-driven security policy from one state to a current state; and

computer program code for determining at the server computer whether a requestor is permitted to access the electronic document, the access being based on a current state of the process-driven security policy, the current state being informed to the server computer by sending the reference to the server computer.